# Hackeři: Kouzlo modré obrazovky

Honza Šípek

28. prosince 2011

**Milují poznání. Řešení logických problémů, zvláště těch nesnadných. Hrají si se stroji všech druhů – ne nutně jen počítačů – hledají v nich slabiny, které nejen využívají, ale také na ně upozorňují a vymýšlejí, jak trhliny zacelit. Zdálo by se, že jsou věčně osamělí před klávesnicí svého počítače, ale mají svou kulturu, skupiny, místa setkávání, folklor i humor. Ale hlavně „svět krásného baudu," jak to kdysi v počítačovém pravěku nazval Mentor ve svém textu Svědomí hackera, též známém jako Mentorův manifest.**

Hackerská kultura usiluje především o svobodu. Kyberspace, prostor, který byl nejdřív zajímavostí pro pár zasvěcených, později novým vesmírem, do nějž se nořili LSD obdaření průzkumníci kontrakultury 60. let, rozvinutým v kyberpunkové odnoži literatury sci-fi (slovo Matrix kupodivu nepochází ze stejnojmenného filmu, ale z knihy Neuromancer Williama Gibsona) pak novým rájem a sférou svobodných informací. Internet však uchvátily Zlé Korporace a Vlády a svobodný prostor se začal zmenšovat. Obranou proti cenzuře je šifrování. Obranou proti uhlazeným a spotřebním obrazovkám Windows je operační systém Linux. Obranou proti všeoblbujícímu klikání a hlazení lesklých obrazovek chytrých telefonů je příkazová řádka. Obranou proti oblbování je vědění.

# Mytologie kyberprostoru

„Máte to vzadu na zahrádce“, vítá nás servírka v plné pražské hospodě, kde se koná jedna z *2600 meetings*, setkání hackerů, jež původně svolával legendární americký časopis 2600, ale dneska se měsíc co měsíc odehrávají po celém světě. Hrkne v nás, že jsme rozpoznatelní na první pohled. Při kyberpunkovém vzezření kolegy Shaddacka se ale venkoncem není co divit. Zahrádka je prázdná. „Promiňte, CO máme vzadu na zahrádce?“ doptávám se servírky. „No přece tu rezervaci,“ pomrkává.

„Máme to tady pravidelně, jsou tu na nás už zvyklí. A vědí, že všichni divný lidi patřej k nám,“ směje se první z příchozích účastníků. Hackeři se trousí jako švábi na pivo. Vyptávající se pisálek jakoby se cítil dílem špiónem, ale i to patří k duchu sešlostí „2k6“, která chtějí být setkáními zájemců o bezpečnost „z obou stran šachovnice“ a termíny i místa se zveřejňují otevřeně na webu.

Vyptávání se po slavných hackerských esech nás vede hluboko do minulosti.

## Kouzlo modré obrazovky

První protohackery (nepočítáme-li Járu Cimrmana, Diviše, sutanu Mendela či bratrance Veverkovy) bychom u nás hledali nejspíš v radioklubech Svazarmu. Komunista chtěl mít pod kontrolou ty, co mohli podnikat něco využitelného ve válce, a založil SVAZARM, Svaz pro spolupráci s armádou. Svazarm měl kluby pro potápěče, kynology, parašutisty, letce, modeláře, ale taky radioamatéry (stavba co nejdokonalejších vysílaček, antén a navazování rádiového spojení na co největší vzdálenost byl tehdy regulérní sport) a později počítačové nadšence. Mnozí vzpomínají na pospolitost při společném bastelní elektronických udělátek, sdílení informací i rad a společné akce – dnes se podobným místů říká *hackerspaces*.

Současně s tím přicházela – i když ve srovnání se západem dost opožděně – další revoluce. Kromě sálových počítačů vyhrazených „strategickým“ a „vážným“ záležitostem – jejichž programy se psaly nejprve na papír, poté pracně děrovaly do papírových děrných štítků a potom si je člověk nechal ve skulině přiděleného strojového času „projet“ a po-

kud došlo k chybě, celý proces se opakoval[1] – se objevily počítače malé, povýtce osobní. Stroje jako ZX Spectrum, Commodore, Atari, Amstrad, či Didaktik, PMD 85, a IQ151 domácí provenience (s výkonem a pamětí zlomku mobilního telefonu, který máte dnes v kapse) si za vzácné valuty mohly pořídit i domácnosti – kdo na ně neměl, mohl se dostat k počítači v osvícenější škole, kroužku domu dětí a mládeže, nebo právě ve Svazarmu.

Kolem malých počítačů začínají vznikat komunity nadšenců. Drtivá většina softwaru byla kradená, neexistoval v podstatě žádný trh, programy a zvláště hry se kopírovaly a vyměňovaly mezi kamarády, na burzách nebo přes inzerát. Pospolitost, směnný obchod. Počítače měly tak malou paměť a programy byly tak krátké, že některé vycházely dokonce v podobě zdrojového kódu v časopisech či knihách[2] – člověk ho prostě z papíru přepsal do počítače a spustil – podobně, jako vycházely specializované časopisy publikující schémata různých elektronických zařízení[3]. Tvořivost a vynalézavost s tím spojená se netýkala jenom psaní vlastních her či programů, ale i upravování programů získaných či odstraňování ochrany proti jejich kopírování – už tehdy![4] A poprvé se dal zahlédnout obraz dnes považovaný za typický: dítě či teenager sedí s planoucíma očima ve ztemnělém dětském pokoji osvíceném pouze obrazovkou počítače – ta naše byla uklidňující modrá Commodoru 64 – a hraje si a zkouší.

## Síť

Ještě než po převratu stihl do země vtrhnout do té doby embargovaný Internet (byli jsme součástí nepřátelského bloku a připojení k původně polovojenské síti USA před rokem 1989 nepřipadalo v úvahu), proje-

[1] u podobných počítačů se tehdy „zašíval“ filosof Jan Sokol či spisovatel Ondřej Neff, který prostředí socialistického výpočetního střediska trefně popisuje v knize *Pole šťastných náhod* (1989).

[2] například pozdější dokumentarista Vít Klusák známý svým *Českým snem* publikoval jako kluk v časopise ABC zdrojový kód hry Videostop

[3] např. časopis *Amatérské rádio* slangově zvaný *Amáro*. Ten mimo jiné věnoval jedno celé číslo schématu na výrobu jednoduchého osobního počítače. Autor tohoto textu začal papírovým modelem a vytahováním se před spolužáky na základní škole, dále se však nedostal.

[4] výbornou studií subkultury osmibitových počítačů včetně kapitoly o tehdejších *crackerech* je kniha *Bludiště počítačových her* (1990) Bohuslava Blažka

vila se touha uživatelů osobních počítačů po vzájemném propojení ve fenoménu zvaném Bulletin Board System neboli BBS. „Bíbíesky“ byly vlastně solitérní počítače připojené pomocí modemu k telefonní lince. Linka byla většinou jedna, člověk se připojil (po tehdejších telefonních spojích, které měly často problém přenést i obyčejný hovor, na několikátý pokus), mohl si stáhnout soubory z „knihovny“, jiné soubory zanechat, případně zanechat vzkaz někomu jinému. V knihovnách bíbíesek se povalovaly hlavně texty (malý objem, nenáročný na přenos) od vědeckých časopisů přes různé návody (často i texty hackerů ze zahraničí; jeden ze spoluautorů této kapitoly napsal za pomoci školní knihovny návod na výrobu jaderné bomby, který publikoval na BBS a který později skandálně „odhalila“ reportáž televize Nova) až po neoficiální překlad Sterlingovy knihy *Zátah na hackery*. Největší proslulosti dosáhla pražská *Infima BBS*, která měla v době svého největšího rozmachu až 32 telefonních linek a umožňovala tedy i simultánní chat několika uživatelů.

Telefonní spojení (pokud bylo meziměsto) bylo drahé a proto se začínají objevovat i návody na tzv. *phone phreaking*, neboli zneužívání telefonní sítě – od způsobů, jak volat zadarmo, návodů na výrobu nekonečných telefonních karet až po servisní kódy umožňující přístup do skrytých služeb telefonní sítě. Nejjednodušším způsobem bylo otevřít rozvodnou skříň a napojit se za pomoci „krokodýlků“ na cizí telefonní linku. To se pak šlo (na cizí účet) dovolat i na zaoceánskou BBS. „Nainstalovali jsme tenkrát jako recesi na jeden telefonní sloup v jakési dědině telefon, přes který se dalo volat zadarmo. Ale do druhého dne zmizel,“ vzpomíná na klukovská *phreakerská* léta jeden z pozdějších hackerů. Jiným z jeho vtípků, že naslepo zkoušel telefonní čísla z budky a dostal se na linku telefonního záznamníku obchodu Tesco. Jen tak zkusil přístupové heslo 1234 a dostal se k možnosti změnit uvítací vzkaz. „Vážení zákazníci, vašich peněz už máme dost, proto jděte do prdele,“ oznamoval pak záznamník překvapeným klientům a druhý den vyšel v novinách článek s titulkem „Utajovaný záznamník už nepromluví.“ Jak uvidíme později, podobně triviální hesla mohou otevřít dvířka nejen do banálních služeb supermarketů, ale i do střežených státních institucí.

## Folklór: Kriminálka není jen tak někdo, jako jó?!

V roce 1992 byla naše kolonie slavnostně připojena k Internetu. Nejprve byly připojeny univerzity a vědecké ústavy a dlouho byl Internet dostupný téměř výhradně ve školních laboratořích. V následujích letech vznikla celostátní síť CESNET, která prozíravě propojila všechny důležitější univerzity a akademická pracoviště, dlouho před tím, než se Internet dostal k běžným jednotlivcům a firmám. Studenti se nořili do okouzlujícího světa propojených informací a komunikace až někam za oceán, zakládali kolejní servery[5], dělali první webové stránky[6]. Ti hloubavější zkoumali, jak to celé funguje a brzy byli chytřejší a schopnější než školní administrátoři. Pronikali do školních serverů a přístupu k nim využívali k různým legráckám. Když došlo na první diciplinární řízení a vyhazovy ze školy, začalo být jasné, že dobrý hacker po sobě musí umět zamést stopy. Ale když se spříznění poznali, zkamarádili se, zakládali různé skupinky bizarních názvů a mejdany na kolejích křížili s hlasitou hudbou a pronikáním do chráněných strojů v hlubinách sítě.

Tříčlenná slovenská skupina SERT měla brzy pod kontrolou desítky „mašin“ nejen v Čechách a na Slovensku, ale i v Maďarsku, Polsku, Finsku a na Taiwanu. Tu a tam vyrazili do boje proti správcům školních serverů, kteří omezovali nebohé studenty, a užili si dost legrace, když sledovali korespondenci zmatených administrátorů, kteří se snažili útok rozkrýt. A občas jim ty maily cestou trošku přepsali, to jen tak, aby věděli. O svém útoku proti administrátorům školních sevrerů, kteří na úkor studentů provozovali úložiště kradeného softwaru, vydali „oficiální“ zprávu za pomoci hacknutého webu slovenské tiskové agentury TASR.

V listopadu 1996 z titulní webové stránky Armády ČR vykoukly nahé zadky děv z pornočasopisu a stránka začala nabízet „informace o Armádě Čínské respubliky, její struktuře, aktivitách, vojenském školství, špionážních akcích, úplatkářských aférách apod.“ Pod stránkou s uklidňujícím nápisem: „Lidi, spěte klidně, nad vámi bdí Armáda České republiky“ byl podepsán voják Švejk. „Hackeři nabourali server armády!“ začalo se psát v novinách a spekulovat o tom, kdo by mohl být

[5] některé pozdější kolejní sítě dosáhly proslulosti až legendární, například síť *Sillicon Hill* na kolejích ČVUT na pražském Strahově

[6] jeden z nich, Ivo Lukačovič, dřívější admin BBS Infima, napsal se spolužákem za prázdniny první verzi webové služby „Seznam.cz“

tajemný CzERT, jenž byl pod útokem podepsán. Ten brzy poskytnul novinářům několik anonymních rozhovorů, v nichž vysvětlil, že se snažil upozornit na skandálně slabé zabezpečení armádního webu a zamezit „potenciálním narušitelům udělat něco strašného“. Následovaly změněné stránky ministerstev (ministerstvo zdravotictví překřtěno na ministerstvo smrti) i firem (Union banka přejmenována na Ruin banku – taky později zkrachovala). Pajkus, ústřední postava CzERTu, založil server Hysteria.sk, který se stal „posledným útočiskem binárných sxizofreniků“. Na „Hysterce“ začal vycházet hackerský „časopis“ Prielom s návody na útoky i filosofičtěji laděnými texty. Archivy hacknutých stránek, záznamy o průnicích, odposlechnuté vtipné emaily adminů, i vlastní texty například o tom, že hacker je nejdarwinističtější tvor, začali sami hackeři schraňovat pod trefným názvem „folklor“.

Folklórní postavou se stal i kapitán Dastych, který se médiím představil jako první český počítačový policista a později začal tvrdit, že je „CzERTovi“ na stopě. Netrvalo dlouho a na webové stránce policie se nezobrazovalo nic než kreslený vtip, na němž jeden policajt říká druhému: „Už jsme tomu hackerovi na stopě, přišli jsme na to, co je to ten Internet!“ [7] Z nahrávky telefonátu kapitána Dastycha, který shánněl údajného hackera v práci, kdosi sestříhal parodickou skladbu, v níž nebožák hláskuje své příjmení a ve smyčce stále opakuje „TVRDÝ Y“ a nesmrtelnou hlášku „kriminálka není jen tak někdo, jako jó!“ Pajkus začal pořádat hackerské srazy, které už byly veřejné. A přestože na „CzERT session“ v Praze (do restaurace rezervované na jméno Dastych) nakonec dorazila policie a všechny přítomné legitimovala, nepodařilo se nikdy nikomu dokázat žádnou trestnou činnost. Major Dastych odešel do civilu. Hackeři na něj vzpomínají s láskou: „Bez něj už to není taková legrace,“ smějou se nad pivem vzadu na zahrádce.

U zrodu další mytologické události stál nápad, který vypadal jako špatný vtip. Z rutinního skenu bezpečnostních děr na síti vyskočila známá chyba v emailovém rozhraní slovenského národního bezpečnostního úřadu. Hackerům chybělo heslo k firewallu instituce (NBÚ SR) a tak z legrace zkusili banální „nbusr123“. Pár příkazů vyťukaných na konzoli a... Kluci za obrazovkami dostali záchvat smíchu. Ono to fungovalo! A když se pokusili získat práva administrátora a server ani

[7] eskapády hackerských skupin SERT a CzERT popisuje detailně kniha *Zásek do živýho* dostupná online http://eldar.cz/kangaroo/zasek_do_zivyho

nechtěl heslo, záchvat smíchu se opakoval. Byli vevnitř.

Hackeři nachytali asi 20GB dat a když díry zůstávaly stále otevřené, zveřejnili chvástavý článek s přesným popisem útoku na doměle nejbezpečnější organizaci v zemi. Začal mediální poprask, admini se začali zmateně bránit, nicméně triviální heslo stále umožňovalo přístup do celé sítě. Fungovalo dokonce i několik měsíců poté, když se začalo prodávat černé tričko s lakonickým nápisem „nbusr123“. A když později policie zabavila „Hysterku“, underground odpověděl dalším odstavením webu NBÚ. Policie byla nad zabaveným strojem bezradná, s žádostí o pomoc se prý obrátila na „bezpečnostní odborníky“ a netušila, že jsou sami členy komunity. „Ale nesázel bych na jejich amatérismus. Oni mají na všechno hlavně hodně času a trpělivosti,“ líčí dnes Pajkus. Právě v Hysterce se našly důležité stopy, které vedly k tomu, že policie obvinila dva slovenské mladíky. Soudy se vlekly roky a po mnohých odvoláních byli oba shledáni nevinnými. Obnovený časopis Prielom vydal text na téma „jak uchránit počítač proti zabavení“ a hackerské srazy „Hysteria Sessions“ se konají dodnes. Nejvíce si prý hackeři užili na tom posledním. Nebylo tam totiž připojení k síti a stihli si konečně popovídat.

Hackeři zestárli, založili rodiny a šli pracovat do bezpečnostních firem, kde je uvítali s doširoka otevřenými náručemi. Větší znalce bezpečnosti těžko najít. Generace kybernetických Jánošíků odrostla a zapojila se do koloběhu samsáry. „Dnešní mladý už nic neuměj,“ vzpomíná nostalgicky nad pivem vzadu na zahrádce jeden z hackerů na zlaté časy Hysterky. Scéna je ale stále živá, jenom se proměnila. Několik z kluků v černých tričkách, kteří tu sedí kolem stolu, má něco společného s prvním českým „hackerspacem“ BRMlab.

## Hackerspaces

Člověk by čekal zapšklé ajťáky ponořené do terminálů, ale v BRMlabu je veselo. Je jedenáct v noci, meetup – každotýdenní setkání všech členů – skončil a a teď je „volná zábava“. K vybavení několika místností v opuštěné kancelářské budově Elektrických podniků na Vltavské, kde pražský hackerspace sídlí, právě přibyl vyřazený plotter a skupinka hackerů se teď baví tím, jak ho rozchodit. „Pingám!“ volá někdo od svého laptopu, „Má to otevřenej port,“ sděluje jiný. Pak spojení zase

padá, obří tiskárna občas zakývne hlavou, valí se vtípky, a všechny to, jak se zdá baví. „Nemáme tak velkej papír," říká někdo. „Tak nevytiskneme si ho?" odpovídá jiný hacker ve zjevné narážce na RepRap, 3D tiskárnu, kterou si v BRMlabu postavili a která narozdíl od běžné tiskárny dokáže vyrábět trojrozměrné předměty jako různé součástky, obroučky na brýle za pětikorunu, nebo sošku Buddhy. Na otázky kolem RepRapu už někteří členové reagují trošku podrážděně: „Děláme tady takovejch zajímavejch věcí a všechny novináře zajímá jenom 3D tiskárna." Není divu, je totiž možné, že právě ona se stane novou revolucí.

Návštěvníky tady nevyhánějí. Když přijde někdo novej, bez ohledu na to, kdo to je, vždycky se ho někdo ujme, představí ostatním a řekne kouzelnou větu: „Však se tady porozhlédni sám." A člověk nevychází z údivu.

Je k půlnoci, ale život tady teprve začíná. Kolem stolů sedí hackeři pohroužení do svých laptopů, ale přesto mezi nimi probíhá živá komunikace. Když někdo něco neví, zakřičí do vzduchu své „Nevíte někdo náhodou...?" a přijde mu odpověď od jednoho z ostatních kluků v černém kolem velikého stolu. Občas proletí vtípek, každý na půl ucha sleduje, co se právě v místnosti děje a podle nálady se od obrazovky odpoutá a zapojí do některého z nekonečných rozhovorů. Možná situace běžná kdekoliv jinde, ale musíme uvážit, že tu sedí undergroundové hvězdy svých oborů. Revezní inženýři, penetrační testeři, programátoři, bezpečáci, fanoušci do elektroniky i lidé zkoumající mozek a jeho biologické projevy. Přes den jsou studenti nebo zaměstnanci počítačových firem. Když se jim člověk zadívá na monitory, narazí většinou na terminál, konzoli, takovou tu černou obrazovku s písmenky podobnou příkazovému řádku, kterého se většina běžných uživatelů počítače děsí. Pro zdejší uživatele Linuxu je ale zadávání příkazů často nejrychlejším způsobem, jak něco udělat, příkazům jde dávat spoustu volitelných parametrů a hlavně: dělat věci, které zdánlivě nejdou.

„Hacker je pro mne především člověk, který je schopen vzít nějakou věc, ať už skutečnou nebo virtuální a použít ji tak jak se obvykle nepoužívá, udělat z ní něco úžasného, obdivuhodného, zajímavého, poučného, je schopen jít dál než je zvykem, je ochoten se od nějaké myšlenky nebo nápadu propracovat k jeho realizaci a dát věcem nějaký, často nový, smysl. Tedy v podstatě specifický případ člověka kreativního," říká Růža, veselý chlapík lehce při těle, nejhovornější z přítomných, a

oči při tom zřídka odlepí od obrazovky.

„Takovej ten v černým tričku...“ popisoval jsem kamarádovi, s kým jsem se v Brmlabu bavil. Rozesmál se. Černý tričko tady má totiž skoro každej, často s podivným logem nebo sloganem, které běžný smrtelník nepochopí.

Vedle to voní kalafunou jako v dávné klubovně Svazarmu. Tady se dělají hardwarové věci, RepRap, 3D tiskárna, právě cosi tiskne a vydává při tom tiché bručení asi jako inkoustová tiskárna. Krabice s různýma součástkama, dráty, tištěné spoje. Vedle je „biolab“, laboratoř na biologické pokusy, kde zatím experimentovali s kvašením, ale pošilhávají i po DNA. Když se člověk začne vyptávat, nadšeně mu ukazují „hračky“ vlastní konstrukce, kterých jsou desítky. Brmlab je zapojen do mezinárodní sítě hackerspaců a kočovní hackeři z celého světa se tu stavují na kus řeči, přespat, přednášet nebo využít vybavení, které jinde nemají. Jako v hackerspacech jinde na světě, i tady najdou basy svého oblíbeného Club Maté, energetického nápoje jednoho německého pivovaru. Z hackerů se stal regulérní městský kmen, tak silný, že se může stát „cílovou skupinou“ pro marketing.

*Autor děkuje za spolupráci Shaddackovi.*

# Rozhovor: Hacker Martin

**Nenechá se fotit. Obezřetně si chrání svoje soukromí. Vyhýbá se jakékoliv narážce, která by ho mohla v úzkém kruhu znalců identifikovat. Má radost, že jsme i text tohoto rozhovoru stylisticky upravili, protože ho nebude možné identifikovat podle jazykových schémat. Na schodech v pološeru noční kancelářské budovy, dlouhá ozvěna a hovor skoro šeptem. Jméno podle toho, jak se zrovna hodí. Nyní Hacker Martin.**

**Můžeš říct, čím se zabýváš?**

Už delší dobu se zabývám počítačovou bezpečností. Primárně různými možnostmi zneužití technologií. A samozřejmě jak zneužití předcházet, abych já osobně nemohl být ovládán.

Je to taková automatika, že když přijdu do styku s novou technologií, první věc, která mne napadne, je, jak by se to dalo využít, hacknout, zneužít. Ani snad ne zneužít, ale kontrolovat, nebo zjistit, jaké tam jsou nezamýšlené souvislosti, které lidi v prvním momentu nenapadnou, ale později vyplavou na povrch.

**Nějakej příklad?**

Třeba chytré telefony jako Android nebo iPhone. První věc, kterou vidí běžní lidé, jsou všechny ty úžasné pestrobarevné aplikace. Mne jako první napadne: teď bude mít jedna společnost pod kontrolou dalších X milionů, miliard, malých počítačů, strategicky rozdistribuovaných mezi lidi. Předtím měli značnou moc – kontrolovali obrovské množství počítačů, provoz na Internetu – a teď se díky těm počítačům/telefonům a jejich senzorům – protože ten telefon má strašně moc senzorů, snad na všechno možné od vibrací, přes polohu, zvuky – dostane o mnoho dále, o mnoho hlouběji.

**Mohou to nějak zneužít?**

Zneužitelnost je obrovská. Mají přístup k obrovskému množství informací. A lidé zdaleka nežijí tak, aby se nedali vydírat, ovlivňovat, kontrolovat. A když máš všechny ty informace a víš, kdy a kde na koho zatlačit, tak můžeš velmi sofistikovaným způsobem, bez použití fyzického násilí, tu společnost ovládat. Informace mají největší cenu. Kdo bude mít informace, ten bude vládnout. S postupujícím technologickým pokrokem je čím dál jednodušší, aby jeden jednotlivec zlikvidoval někoho jiného. Ochrana proti tomu je, když nemají dost informací o tom,

jak společnost funguje, kdo jsi ty. Nevědí, koho mají zlikvidovat. Čím víc informací máš, tím líp víš, proti komu bojuješ. Nebo kde máš zatlačit, abys tu společnost ovládl.

Všichni politici, kteří teď vyrůstají, všechny jejich aktivity jsou zaznamenané. Každý dotaz někde na Googlu nebo každý profil na Facebooku. A jednoho dne ti lidé dozrají, dostanou se do stádia, kdy se z nich budou vybírat noví politici nebo policajti. Je v podstatě jedno, kdo se tím politikem stane, vždycky na něj budeš něco vědět.

Dneska ti Google z jednoho mailu leze do vyhledávání, do sociálních sítí a do mobilu, za chvíli ti bude lízt všude. Nekoupíš si normální počítač, koupíš si počítač s operačním systémem Google a všechno budeš mít online. Možná s výraznou slevou, nebo ti budou dávat hardware za symbolickou cenu – v každém případě budou pronikat dál a dál.

**Máš z toho strach?**

To není o strachu. Tak to evolučně bude fungovat. Jediná možnost pro ty mocenské struktury, které se evolučně udrží, je, že se nebude vědět, kdo jsou – právě anonymita. To, že vyhrají takovíhle lidé, neznamená, že budou horší než ti, co vládnou teď. Kdyby měli dostatečně silné morální postoje, mohlo by to být v principu lepší. Tím, že se ty metody zjemňují, mohlo by se zabránit ohromnému množství zbytečného násilí.

**Jak si představuješ svět za patnáct let?**

Bude posilovat element vlivu korporací, centralizace informací.

**Jak se bráníš?**

Já se snažím žít tak, abych co nejméně podléhal tomu tlaku na vysávání informací, tzn. abych neměl email někde na Gmailu, abych jim nedával všechnu svoji souborovou historii, abych se anonymizoval, abych měl vlastní server, ne nějaký virtuální někde v nějakém cloudu, o kterém nevím, kdo k němu má ještě přístup, abych měl zašifrovaný disk, abych používal šifrovanou komunikaci se všemi, atd. V praxi to samozřejmě nedodržuju na 100 %, někdy jsem pohodlný. Je to těžší cesta, když si děláš všechno takhle sám. Stojí tě to hodně námahy, máš evoluční podmínky o dost těžší, protože nemůžeš dělat to, co chceš, musíš trávit čas jenom údržbou těch prostředků.

Jestli je pravda, že informace mají největší cenu, potom vlastně tím, že o tobě nebude tolik informací k dispozici, tak bys měl být pseudosvobodnější. Je otázkou jestli doopravdy.

**Jaký vliv budou moci mít jednotlivci ve společnosti, kde bu-**

**dou vládnout koncentrované informace?**

Jsi stále víc závislejší na těch technologiích, a to nejenom nadbytkem, volným časem, ale i samotnou existencí. Už to není tak, že můžeš žít bez nich, a s nimi lépe. Už se dostáváš do stádia, kdy bez nich nemůžeš žít, protože by se ti to celé zhroutilo. To dává lidem, kteří umí technologie kontrolovat – například to zařízení hacknout – obrovskou moc.

Pár schopných hackerů ti dokáže položit celý stát. Udělat velké věci. Miliarda lidí může být nahrazena stovkou schopných, motivovaných, dobře organizovaných lidí. Ani nemusí mít tolik prostředků. Závisí to hlavně na vědění, tak s jedním obyčejným počítačem můžeš udělat obrovské věci.

Čím chceš být lepší, tím víc to od tebe vyžaduje disciplíny, musíš se učit, nesmíš zlenivět, nesmíš zblbnout – což se některým lidem stává – nesmíš to přestat řešit, musíš stále jít dál dál dál… ale za předpokladu, že všechno z toho zvládáš, můžeš mít větší vliv než milión vojáků.

Když si nějaký takový jednotlivec myslí, že je něco špatně, má obrovskou možnost udělat změnu. Má jeden výstřel, jednu šanci. Možná víc, ale minimálně jednu. A tu jednu nejsou schopni předpovědět. Vědí statisticky, že je tu tisíc lidí, kterým se něco nelíbí, a jeden nebo dva z nich vystřelí. Ale nevědí, kdo. A je tu tedy naděje, že i když společnost bude někdo oblbovat, tyranizovat, budou stále lidi, kteří řeknou: NE.

**Jak se vyhrabat dost vysoko, aniž bys ztratil anonymitu?**

Dostat se vysoko ve smyslu, kolik toho umí, kolik počítačů nebo zařízení dokážou ovlivnit. Podle mne to možné je, myslím si, že takoví lidé jsou, některé z nich myslím znám – anebo si myslím, že znám, to těžko říct – ale jsou. Když například dokážeš v jeden okamžik hackout tisíc billboardů, ovlivníš veřejné mínění. Ale když to samé uděláš s dopravním systémem, dokázal bys zablokovat dopravu, kdybys dokázal ovlivnit přenosovou soustavu, tak umíš zkolabovat elektrárny nebo továrny. A čím dále jdeš, tím víc věcí dokážeš ovlivnit. Samozřejmě to stojí víc disciplíny a všeho ostatního. Myslím si, že je reálně možné, aby jeden člověk, kdyby se nad tím pořádně zamysel, by dokázal na pár dní paralyzovat celý stát. Stroje natolik pronikly do společnosti, že to možné je.

**A ty znáš někoho, kdo by uměl hacknout rozvodnou síť?**

Já se obávám, že tyto věci jsou mnohem jednodušší, než si většina

lidí myslí. Myslím si, že lidí, kteří by to zvládli, jsou řádově stovky nebo dokonce tisíce.

**Celosvětově?**

U nás. Já osobně jsem osobně jsem se dostal k nějakým technologiím, o kterých jsem si předtím myslel, že musí být bezpečné. Klíčové věci, to už musí být extra třída zabezpečení. Ale zjistil jsem, že těch věcí, které jsou dělané úplně špatně je strašně moc. A fungují na nich skutečně kritické věci. Které když ti vypadnou, tak může nastat chaos ve společnosti.

**Byl's už někdy vevnitř v něčem takovým?**

[Mlčení. A lehký úsměv.]

**Není člověk v pokušení?**

[Mlčení. A smích.]

**Jakej druh pocitů člověk při pronikání do mašin zažívá?**

Samozřejmě nějakou roli tam hraje i ego: mám na to. Je to do značné míry zábava. A do obrovské míry zvědavost. Například díky té zvědavosti jsem se dostal k hromadě informací o mně, které jsem asi nikdy vidět neměl. Takové věci, které tě obrovským způsobem ovlivní. Začneš vnímat svět úplně jinak.

Samozřejmě je tam vždycky riziko, že tomu podlehneš, že to začneš ve velkém zneužívat – já osobně jsem si stanovil zásadu, že nikdy z toho nesmím mít žádný finanční profit. Za žádných okolností. Ani že bych využil informací, které získám, například k tomu, že bych si založil nějaký byznis. Nic. V momentě, kdy z toho máš peníze, už to nedokážeš zastavit. Znal jsem lidi, kteří se takhle zkurvili. Nejdřív jenom tak trošku a pak zjistili, že už nedokážou fungovat jinak.

Stejně tak se snažím nečumět lidem – a hlavně těm blízkým – do soukromých věcí.

**Jde to říct nějak konkrétněji?**

Dejme tomu, že pozoruješ nějaké chování, které ti nesedí, pozoruješ, že se lidi kolem tebe začínají chovat nějak jinak, a snažíš se zjistit, čím to je. Něco se děje. Nevíš proč. A víš, že by ses mohl podívat někam, kde to najdeš. Ale snažíš se to neudělat, protože to není správné. Potom bys to začal dělat stále znova a všude.

**Jakým způsobem ti to, co ses o sobě dozvěděl, změnilo pohled na svět?**

Začneš chápat širší souvislosti. Nějací lidé kolem tebe něco dělají, ale zjevně je za tím něco organizovaného, něco, co nevidíš. Ale zapama-

tuješ si to. Pak se dostaneš k informacím a zjistíš, jak ty mechanismy fungovaly. Zjistíš, že jsi byl někým využitý, nebo že jsi součástí něčeho většího, co se někam hýbe, co tě jenom nějak „vhodně“ směruje, abys něco dělal.

**Jak se tady dá rozlišit mezi náhodným chováním a úmyslem? Jak zůstat bdělý, ale nepřekročit paranoiu?**

Těžko. Hodně lidí si o mne myslí, že jsem paranoidní. Částečně možná i mají pravdu. Navzdory tomu vím, co vím. Už jenom díky tomu, že vím, jak pracujeme my, když něco chceme zjistit, nebo když mne něco zaujme nebo naštve, nebo prostě když ty informace chci. Vím, jak by postupoval někdo, kdo by chtěl to samé udělat mne. Možná to je stejně jako s těmi mafiány: stále se bojí, že je někdo zastřelí, protože oni sami chodí a střílí lidi. Ale těžko říct.

Jedno pravidlo, kterým se řídím, je, že nikdy – no nemůžu říct, že bych nikdy nepřekročil zákon, když jsem byl děcko, dělal jsem toho spoustu – ale zpětně můžu říct, že jsem nikdy neudělal nic, co bych zpětně považoval za nemorální. Možná někdo jiný by to nepovažoval za morální, ale vnitřně jsem konzistentní. Nikdy jsem neuškodil nikomu pseudonevinnému – i když nemám právo vynášet nějaké soudy.

**Jak dlouho se bezpečností zabýváš, jak ses k tomu dostal, co byly původní impulsy?**

Zabývám se tím… vlastně kam moje pamět sahá. Když jsem začal dospívat, v nějakých 14 letech, to zcela jistě. Předtím jsem měl tu touhu, ale nic jsem neuměl. A jak jsem rostl, tak to začalo růst. Je spousta lidí, které bavilo to samé, spousta z nich byla lepší než já – o hodně lepších – ale potom si našli jiné zájmy, přestalo je to bavit, nebo začali dělat něco jiného.

Dost důležitá je podle mého disciplína. Člověk si řekne, že některé věci nedělá a jiné naopak dělá, systematicky, dlouhou dobu.

**A co je to, co děláš systematicky?**

Například, že se stále vzdělávám, stále hledám nové věci, snažím se nezakrnět, jít stále hlouběji, dále, víc...

Je jedno, jaký je to konkrétní problém. Naučíš se podívat na ten problém, nějak si ho logicky zanalyzovat, když to nefunguje a není jiná možnost, tak jdeš na nižší a nižší úroveň, až prostě tu chybu najdeš a potom zase zpátky... tak ten přístup funguje víceméně na všechno. Musíš mít dostatečný tah na bránu, cílevědomost. Spousta lidí je šikovná, má nápady, ale když narazí na nějaký problém, zkusí to jen párkrát,

zjistí, že to nejde a vykašlou se na to.

**Má to i rysy závislosti?**

Já se obávám, že to je povahový rys. Napůl je to cílevědomost – chci, chci, chci – třeba něco dodělat. A napůl nechci a neumím přestat, neumím se od toho odtrhnout. Taková zarputilost. Někdy je to výhoda, že to neděláš polovičatě a jdeš dál, dál, dál, někdy je to nevýhodné, že se namotáš na nějaký hodně složitý problém. Taky můžeš takhle padnout do pasti.

**Jak vypadá současné kyberpodsvětí?**

Příjmy z internetové kriminality jsou v současné době už větší, než příjmy z obchodu s drogami. VISA veřejně uvádí, že nějaká 2 % ze všech transakcí jsou podvody. Odhaduje se ale, že to je i víc.

Vytváří se společenská třída, která žije z těchhle peněz, která je dostatečně inteligentní, která má dostatečně anonymní zdroje. Z této činnosti dostává řádově vyší finance, než dostávají tajné služby. Mají proti sobě organizaci – nazvěme ji mafie – která má spoustu zdrojů, která má schopné lidi, a mají proti ní bojovat. Musí prohrát.

**Víš anebo tušíš, že takové organizace existují?**

Viděls někdy černou díru? Neviděl. Ale z toho, že se to okolí nějak chová, umíš odhadnout, že tam něco musí být. Nemůže se to jenom tak ztrácet, někde se to musí koncentrovat. To, že tu strukturu nevidíš, je jedna věc, ale víš, že tam někde bude.

## Autor

**Honza Šípek** – filmový dokumentarista, z okouzlení hackerskou komunitou napsal na gymnáziu knihu *Zásek do živýho* (online na http://eldar.cz/kangaroo/zasek_do_zivyho), později s kamarády založil server Eldar.cz, o který se stará. Pět let pracoval v internetovém rádiu Akropolis, během studia na FAMU natočil film *Souboj s mozkem* (http://eldar.cz/mozek), jehož jedním z protagonistů je hacker Shaddack. Společně na základě filmu připravují *Nebezpečnou knihu* s podtitulem *Umění digitální války* (http://eldar.cz/kniha).

**Tento text je rozšířenou verzí kapitoly „Hackeři“, která vyšla v knize o městských subkulturách s názvem *Kmeny* v roce 2011.**